PhD/M.Sc. Engg. CSE 08 December 2023 (Afternoon) 51

# ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

## Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION WINTER SEMESTER, 2022-2023
DURATION: 3 HOURS FULL MARKS: 150

## CSE 6251: Cryptography

**Programmable calculators are not allowed. Do not write anything on the question paper.**
Answer **all 6 (six)** questions. Figures in the right margin indicate full marks of questions.

1. a) What do you understand by cryptanalysis of a system? How does cryptography differ from steganography? 5

   b) Briefly explain the cryptographic strength of Vigenere cipher over playfair cipher. Using the Vigenere cipher encrypt the word “"unfaithful” using the key ‘thief’. 8

   c) Why AES is not a Feistel algorithm? Draw the block diagram of AES Encryption and Decryption process. Briefly explain the Mix Columns step used in each round of AES. 12

2. a) Cipher Block Chaining (CBC) and Electronic Code Block (ECB) are two modes of operation for block ciphers. What is the limitation of ECB and What are the solutions proposed to provide both integrity and privacy in CBC? 8

   b) Revocation of public key certificates is an important part of PKI. But certificates also carry expiration dates, so there are two ways in which a certificate can be invalidated (revocation and expiration). What are the reasons for having two ways of invalidating certificates? Would it not be sufficient with revocation? 10

   c) Design a two-message authentication protocol, assuming that Alice and Bob know each other's public keys, which accomplishes both mutual authentication and establishment of a session key. 7

3. a) Alice wants to use RSA to encrypt the message $M = 88$ and send it to Bob. Bob has chosen two prime numbers ($p = 17$ and $q = 11$) to calculate the public number needed for the RSA keys. Furthermore, Bob has selected the number $e = 7$ to use in his public key.

      i. What is the private key and resulting public key published by Bob? 4

      ii. What is the resulting ciphertext block C that Alice with send to Bob using RSA to encrypt her message ($M = 88$)? 4

   b) Assume that you are developing code that is digitally signed by a trusted software distributor before let out on the market. They will examine the source carefully and only sign (using SHA-1) the binary code that they will compile given your source code. How is the signing done? How could you exploit (assuming you're an evil hacker) the crack in SHA-1 to fool them to sign your trojan horse that will take over the world? 10

   c) With the aid of a diagram show the authenticated Diffie-Hellman key exchange. Why Deffie-Hellman algorithm is considered as public key cryptography? 7

4. a) Several countries are introducing passports with a built in RFID chip. The chip is passive but will reply when read by a radio scanner. The distance between the chip and the scanner is of course up to the scanners signal strength and size of antenna. The chip that will be used in passports can typically hold 64 Kbyte of data, most probably information such as name, date of birth, photo, other biometric data etc. The idea is that a customs officer can quickly get all the information he needs to identify you. There are several problems that must be solved. As an security expert answer the following question:

      i. How it can be ensured that, the information stored on the chip is correct? 4

ii. If anyone can program a chip, he/she could claim to be Batman. How would you design a system so that a customs officer, in a different country with no network connections, could validate the information? 5

iii. If anyone can scan your passport they would also know all your personal information. One proposed solution is to print a key, using a bar code, inside the passport. Only the one who can see the bar code will then be able to interpret the information on the chip. How would this work? What encryption technique could be used? 6

iv. Assuming that the chip is very simple and replies with the same data every time it is probed, what threats to privacy do we have even if we cannot interpret the reply? 5

b) Why is it easy for the good guys to find a big prime number? Why is difficult for the bad guys factorizing a big number? 5

5. a) Kerberos is a protocol that is based around Needham- Schroeder protocol for many to many authentications. Now answer the following questions. (Use necessary diagrams to justify your answers) $3 \times 5$

i. What is the main idea behind the use of a TGT (Ticket Granting Ticket)?

ii. Why the network layer address is included in the ticket in Kerberos V4?

iii. The information in a TGT (Ticket Granting Ticket) is encrypted so the client cannot access the information in the TGT. However, all information in the ticket is already known to the client. Why is it still necessary to encrypt it?

b) Design a variant of Kerberos in which the workstation generates a TGT. The TGT will be encrypted with the user's master key rather than the KDC's master key. How does this compare with standard Kerberos in terms of efficiency, security, etc.? What happens in each scheme if the user changes her password during a login session? 10

6. a) Your company (SECURELINK LTD.) is responsible of the security design of an online banking website (TRUSTED BANKING). The new system, known as (SAFEGUARD), should allow every registered customer to check the status of their bank account and perform secure online bank transfers. Your company receives a set of requirements for the new design that can be summarized in five categories: $5 \times 5$

i. Protection against denial of service attack (DoS) to the bank web server (Trusted Banking). (i.e. Trudy cannot overload the web server by sending multiple fake web requests)

ii. Strong authentication of the Bank's customers. (i.e. Trudy cannot impersonate Alice)

iii. Privacy and integrity of the communications between the TRUSTED BANKING and the customer. (i.e. Trudy cannot read or modify the content of the communications between the Bank's server and Alice)

iv. Strong authentication of the Bank's website (i.e. Trudy cannot impersonate the Bank's website. Alice is sure to be talking to the Bank)

v. The bank can prove to the customer and to any other third party (e.g. tax authorities) that certain bank transfer has been performed in some given time. (i.e. Trudy cannot create a fake invoice. Strong accountability.)

In order to avoid money laundry, every year the bank sends to each customer and to the tax authorities a written summary of every bank transfer performed from the account. Describe how your new SAFEGUARD will work. Write how you will provide each of the five features in a different section/paragraph.